REMARKS

This response is submitted in reply to the Office Action dated September 22, 2005. Claims 13 – 23 were rejected under 35 U.S.C. 112 and claims 1 – 23 were rejected under 35 U.S.C. 103. In response, Applicants have amended claims 1, 5, 13, 14, 21, 22 and 23 to clarify the claim language and to advance the prosecution of this Application. No new matter has been introduced as a result of the amendments. Applicants respectfully traverses the rejections. Favorable reconsideration is requested.

Claims 13, 14, 21, 22 and 23 and the intervening claims were rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description. Applicants respectfully disagree with such, but in an effort to further the prosecution of the application to fully cooperate with the Patent Office, Applicants have amended such claims to eliminate the claim language that allegedly fails to comply with 35 U.S.C. 112, first paragraph. Accordingly, Applicants respectfully submit that the rejection of claims 13, 14, 21, 22 and 23 and the intervening claims is now moot and therefore respectfully request that such rejection be withdrawn.

Claims 1-23 were rejected as being unpatentable over U.S. Patent No. 6,694,436 to Audebert ("Audebert"). Applicants respectfully traverse this rejection, as the cited reference fails to disclose or suggest the features claimed in the present invention. Favorable reconsideration is respectfully requested.

Of the claims pending, claims 1, 5, 13, 14, 21, 22 and 23 are the sole independent claims. Claim 1 is directed to a user authentication system, including: a data holding medium for holding a common key unique to a user, used in a common-key encryption method for authentication between the data holding medium held by the user and an authentication apparatus, and a private key used in a public-key encryption method to the authentication between the data holding medium and a server to perform a service to the user; said authentication apparatus for holding the common key used in the common-key encryption method and a private key used in a public-key encryption method, each unique to the user; and an information processing apparatus connected to the authentication apparatus in an always-communicable manner and provided with a function for performing authentication by the public-key encryption method; wherein the authentication apparatus performs authentication, authenticating the data holding medium by using the common key used in common-key encryption method for the user held by the data

holding medium, in response to an authentication request sent from the information processing apparatus, and, only when the user has been authenticated, performs processing for making the information processing apparatus authenticate the user by using the private key corresponding to the user, wherein information encrypted by the public-key encryption method is sent from the information processing apparatus, forwarded to the authentication apparatus, decrypted using the private key corresponding to the user so as to obtain decrypted information; wherein the decrypted information is encrypted means using the common key; and wherein the obtained common key encrypted information is sent back to the data holding medium.

Claim 5 is directed to a user authentication method for a user who carries a data holding apparatus for holding a common key unique to a user, used in a common-key encryption method for authentication of the data holding apparatus held by the user and an authentication apparatus for authentication between the data holding apparatus and a server to perform a service to the user, the method including the steps of: authenticating the data holding apparatus of the user by the common-key encryption method by using the common key held by the data holding apparatus in response to an authentication request from the server; and performing, only when the user has been authenticated, processing for authenticating the user by a public-key encryption method.

Claim 13 is directed to an authentication method, including the steps of: holding a common key unique to a user used in a common-key encryption method for authentication between a data holding apparatus held by the user and an authentication apparatus, and a private key used in a public-key encryption method to the authentication between the data holding apparatus and a server to perform a service to the user; authenticating, in response to an authentication request sent from an external information processing apparatus, the data holding apparatus by using the held common key used in the common-key encryption method for the user held by the data holding apparatus; and performing, only when the data holding apparatus has been authenticated in the authentication step, processing for making the information processing apparatus authenticate the data holding apparatus by the public-key encryption method by using the private key corresponding to the user, wherein information encrypted by the public-key encryption method is sent from the server, forwarded to the authentication apparatus, decrypted by an authentication device using the private key corresponding to the user so as to

obtain decrypted information; wherein the decrypted information is encrypted means using the common key; and wherein the obtained common key encrypted information is sent back to the data holding apparatus.

Claim 14 is directed to an authentication apparatus, including: a holder for holding a common key unique to a user, used in a common-key encryption method for authentication between a data holding medium held by the user and an authentication apparatus, and a private key used in a public-key encryption method to the authentication between the data holding medium and a server to perform a service to the user; an authenticating device for, in response to an authentication request sent from the server, authenticating the data holding medium by using the common key used in common-key encryption method for the user held by the data holding medium, and for, only when the data holding medium has been authenticated, by using the common keys, performing a processing for authenticating between the data holding medium and the server by using the private key corresponding to the user, wherein information encrypted by the public-key encryption method is sent from the server, forwarded to the authentication apparatus, decrypted by the authentication device using the private key corresponding to the user so as to obtain decrypted information; wherein the decrypted information is encrypted means using the common key; and wherein the obtained common key encrypted information is sent back to the data holding medium.

Claim 21 is directed to a user authentication system, wherein a data holding medium for holding a common key unique to a user, used in a common key encryption method, including: a server for sending an authentication request to perform a service to the user; and an authentication apparatus comprising, a holding means for holding the common key used in a common-key encryption method for authentication between a data holding medium held by the user and the authentication apparatus, said holding means holding a private key used in a public-key encryption method to the authentication between the data holding medium and the server; means for authenticating the data holding medium by using the common key used in common-key encryption method for the user held by the data holding medium in response to the authentication request sent from the server, said authenticating means performing a processing for authentication between the data holding medium and the server by using the private key corresponding to the user when the data holding medium has been authenticated by using the

common keys, wherein information encrypted by the public-key encryption method is sent from the server, forwarded to the authentication apparatus, decrypted by the authentication device using the private key corresponding to the user so as to obtain decrypted information; wherein the decrypted information is encrypted means using the common key; and wherein the obtained common key encrypted information is sent back to the data holding medium.

Claim 22 is directed to an authentication method between a data holding medium and a server by an authentication apparatus, said data holding medium holding a common key unique to a user, used in a common-key encryption method, wherein said authentication apparatus holds the common key and a private key used in a public-key encryption method, the authentication method including the steps of: authenticating, in response to an authentication request sent form the server to perform a service to the user, the data holding medium by using the common key used in common-key encryption method for the user held by the data holding medium, and for, only when the data holding medium has been authenticated, by using the common keys; and performing a processing for authentication between the data holding medium and the server by using the private key corresponding to the user when the data holding medium has been authenticated by using the common keys, wherein information encrypted by the public-key encryption method is sent from the server, forwarded to the authentication apparatus, decrypted by the authentication device using the private key corresponding to the user so as to obtain decrypted information; wherein the decrypted information is encrypted means using the common key; and wherein the obtained common key encrypted information is sent back to the data holding medium..

Claim 23 is directed to an authentication apparatus, including: a holding means for holding a common key unique to a user, used in a common-key encryption method for authentication between a data holding medium held by the user and the authentication apparatus, said holding means holding a private key used in a public-key encryption method for authentication between the data holding medium and a server to perform a service to the user; means for authenticating the data holding medium by using the common key used in common-key encryption method for the user held by the data holding medium, and for, only when the data holding medium has been authenticated, by using the common keys, in response to the authentication request sent from the server, said authenticating means performing a processing

for authentication between the data holding medium and the server by using the private key corresponding to the user when the data holding medium has been authenticated by using the common keys, wherein information encrypted by the public-key encryption method is sent from the server, forwarded to the authentication apparatus, decrypted by the authentication device using the private key corresponding to the user so as to obtain decrypted information; wherein the decrypted information is encrypted means using the common key; and wherein the obtained common key encrypted information is sent back to the data holding medium.

In contrast to the claim language, and as previously discussed, Audebert fails to teach, suggest or disclose, the claimed limitations of the presently pending application. At a minimum, Audebert fails to teach, suggest or disclose, in part, holding a common key unique to a user used in a common-key encryption method for authentication between a data holding apparatus held by the user and an authentication apparatus, and a private key used in a public-key encryption method to the authentication between the data holding apparatus and a server to perform a service to the user, as fully supported by the Specification, for example at page 2, lines 21-25 and page 12, lines 17-29. In contrast, Audebert is directed to a transaction that is signed by the terminal module using a private key held by a card. See, Audebert, column 21, lines 28-30.

Further, Audebert fails to teach, suggest or disclose, in part, wherein information encrypted by the public-key encryption method is sent from the server, forwarded to the authentication apparatus, decrypted by the authentication device using the private key corresponding to the user so as to obtain decrypted information; wherein the decrypted information is encrypted means using the common key; and wherein the obtained common key encrypted information is sent back to the data holding medium, as fully supported in the Specification. See, for example, Specification, page 11, lines 9-28. In contrast, Audebert is directed to an exchange where the terminal module decrypts the private key, signs the transaction by means of the private key, destroys the private key and sends the signed transaction to the PC which sends the transaction to the server. See, Audebert, column 22, lines 7-10. Therefore, for at least these reasons, Applicants believe that Audebert is distinguishable from the claimed invention.

Accordingly, Applicants respectfully request that the anticipation rejection with respect to claims 1-23 be reconsidered, and, thus, the rejection be withdrawn based on at least the reasons discussed above.

Respectfully submitted,

BY _____

Thomas C. Basso
Reg. No. 46,541
Customer No. 29175

Dated: December 7, 2005

This Page is Inserted by IFW Indexing and Scanning Operations and is not part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☐ **FADED TEXT OR DRAWING**
- ☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☑ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.